IN THE CLAIMS:

The following listing of claims is presented for the Examiner's convenience. No claims have been amended, added, or cancelled in this response.

1-30. (Cancelled)

31. (Previously presented) A method of operating a file server, said method including:

identifying a file on said file server as using a first security style selected from among a plurality of security styles corresponding to a plurality of security styles implemented on said file server; and

mapping access control limits in another one of said plurality of security styles into said first security style, comprising performing static mapping for validation of said access control limits for said file and performing dynamic mapping for reading or modification of said access control limits for said file.

32. (Previously Presented) A method as in claim 31, wherein said plurality of security styles includes a Windows NT security style.

33. (Previously Presented) A method as in claim 31, wherein said plurality of security styles includes a Unix security style.

34. (Previously presented) A method as in claim 31, further comprising enforcing said first security style for all accesses to said file including accesses in another one of said plurality of security styles;

wherein said enforcing step enforces said security style for all accesses to the file regardless of the security style associated with the entity who seeks access to the file.

35. (Previously presented) A method as in claim 31, including:

associating said file with a subset of files in a file system; and

limiting said subset of files to a security subset of said plurality of security style; wherein attempts to set permission in said subset of files are restricted to said security subset.

36. (Previously Presented) A method as in claim 35, wherein said security subset includes a Windows NT security style.

37. (Previously Presented) A method as in claim 35, wherein said security subset includes a Unix security style.

38. (Previously presented) A method as in claim 35, further comprising caching associations and limits for the subset of files for future use.

39. (Cancelled)

40. (Previously presented) A method as in claim 31, further comprising identifying said file with a second security style selected from among the plurality of security styles in response to a file server request.

41. (Previously presented) A method as in claim 40, including associating said second security style with a file server request for setting permissions for said file when said file server request is successful.

42. (Previously Presented) A method as in claim 40, wherein said file is associated with said second security style regardless of the security style previously associated with said file.

43. (Previously presented) A file server including:

a set of files available on said file server, each of said files having an associated security style selected from among a plurality of security styles corresponding to a plurality of security styles implemented on said file server;

wherein said file server maps access control limits among said plurality of security styles, comprising performing static mapping for validation of said access control limits for said file and performing dynamic mapping for reading or modification of said access control limits for said file.

44. (Previously Presented) A file server as in claim 43, wherein said plurality of security styles includes a Windows NT security style.

45. (Previously Presented) A file server as in claim 43, wherein said plurality of security styles includes a Unix security style.

46. (Previously Presented) A file server as in claim 43, including

a subtree of files in said file system associated with a security subset of said plurality of security styles;

wherein said file server restricts attempts to set permissions in said subtree to said security subset.

47. (Previously Presented) A file server as in claim 46, wherein said security subset includes a Windows NT security style.

48. (Previously Presented) A file server as in claim 46, wherein said security subset includes a Unix security style.

49. (Previously Presented) A file server as in claim 43, wherein said file server is capable of altering the security style associated with said file in response to a file server request.

50. (Previously Presented) A file server as in claim 49, wherein said file server is capable of altering the security style associated with said file in response to a file server request when said file server request is successful.

51-56. (Cancelled)

57. (Previously presented) A method as in claim 31, further comprising enforcing said first security style for all accesses to said file including accesses in another one of said plurality of security styles;

wherein enforcing further comprises translating a user identification associated with said accesses to said first security style.

58. (Previously Presented) A file system as in claim 43, wherein said file server enforces said associated security style for all accesses to said file including accesses in another one of said plurality of security styles by translating a user identification associated with said accesses to said associated security style.

59. (Previously presented) A method as in claim 31, further comprising enforcing said first security style for all accesses to said file including accesses in another one of said plurality of security styles;

wherein enforcing further comprises making a translation of an access control list to access permissions; and

further comprising caching said translation.

60. (Previously Presented) A file server as in claim 43, wherein said file server enforces said associated security style for all accesses to said file including accesses in another one of said plurality of security styles;

wherein enforcing said associated security style comprises making a translation of an access control list to access permissions; and

wherein said file server caches said translation.

61. (Previously Presented) The method of claim 31, wherein dynamic mapping comprises mapping access control limits in said another one of said plurality of security styles into said first security style at a time the mapping of access control limits is required.

62. (Previously Presented) The method of claim 31, wherein static mapping comprises mapping access control limits in said another one of said plurality of security styles into said first security style at a time the said another one of said plurality of security styles is established.

63. (Previously Presented) The method of claim 31, wherein dynamic mapping comprises mapping access control limits in said another one of said plurality of security styles into said first security style at a time the mapping of access control limits is required and static mapping comprises mapping access control limits in said another one of said plurality of security styles into said first security style at a time the said another one of said plurality of security styles is established.

64. (Previously Presented) The file server as in claim 43, wherein dynamic mapping comprises mapping access control limits in said another one of said plurality of security styles into said first security style at a time the mapping of access control limits is required.

65. (Previously Presented) The file server as in claim 43, wherein static mapping comprises mapping access control limits in said another one of said plurality of security styles into said first security style at a time the said another one of said plurality of security styles is established.

66. (Previously Presented) The file server as in claim 43, wherein dynamic mapping comprises mapping access control limits in said another one of said plurality of security styles into said first security style at a time the mapping of access control limits is required and static mapping comprises mapping access control limits in said another one of said plurality of security styles into said first security style at a time the said another one of said plurality of security styles is established.